UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/579,311	05/16/2006	Adolf Proidl	AT 030063	1721

24737 7590 07/07/2009
PHILIPS INTELLECTUAL PROPERTY & STANDARDS
P.O. BOX 3001
BRIARCLIFF MANOR, NY 10510

EXAMINER	
WELLS, ALEXIS M	

ART UNIT	PAPER NUMBER
3621	

MAIL DATE	DELIVERY MODE
07/07/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/579,311	PROIDL, ADOLF	
	Examiner	Art Unit	
	ALEXIS WELLS	3621	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 May 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-17* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-17* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *16 May 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☒ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Status of Claims

1. This action is in reply to the Application filed on 05/16/2006.

2. Claims 1-17 are currently pending and have been examined.

Priority

3. Receipt is acknowledged of papers submitted under 35 U.S.C. 119(a)-(d), which papers have been placed of record in the file.

Claim Objections

4. Claim 14, 16 objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form.

Claim Rejections - 35 USC § 112

1. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2. Claims 1-17 rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The claims are replete with errors. Some examples follow:

a. In claims 13-14, it is unclear whether Applicant is claiming the subcombination of a data-sink device (3) or the combination of a device (2) and a data-sink device (3). If it' s Applicant' s intent to claim only the subcombination, the body of the claims must be amended to remove any positive recitation of the combination. If it is Applicant's intent to claim the combination, the preamble of the claim must be amended to be consistent with the language in the body of the claim. For the latter, the Examiner recommends claiming "A system."

b. In claims 15-16, it is unclear whether Applicant is claiming the subcombination of a data-source device (4) or the combination of a device (2) and a data-source device (4). If it' s Applicant's intent to claim only the subcombination, the body of the claims must be amended to remove any positive recitation of the combination. If it is Applicant's intent to claim the combination, the preamble of the claim must be amended to be consistent with the language in the body of the claim. For the latter, the Examiner recommends claiming "A system."

c. In claim 17, it is unclear whether Applicant is claiming the subcombination of a combination device (24,25) the combination of a data-source device (4), a data-sink device and device (2). If it' s Applicant's intent to claim only the subcombination, the body of the claims must be amended to remove any positive recitation of the combination. If it is Applicant's intent to claim the combination, the preamble of the claim must be amended to be consistent with the

language in the body of the claim. For the latter, the Examiner recommends claiming "A system."

d. Claim 17 recites the limitation "data-source device as claimed in claim 13." Claim 13 is directed to a "data-sink device." It is unclear what the applicant is referencing in claim 13. Appropriate clarification or correction is required.

e. Claims 1-17 contain inconsistent terminology in the claims rendering the claims indefinite. Claims 1-17 contain reference characters including numbers and letters for example, *(DI, D2; DI' D2')* and *(BLI, BL2; BLI', BL2')*. These reference characters render the claims indefinite since they correspond to 'sets of digital data' and 'sets of authorization-to use-information' but are not claimed in this way. Appropriate clarification and correction is required.

f. Claim 13 is directed towards a data-sink device for using digital data, however, it is dependent on claim 7 which is a device (2) for preventing unwanted use of digital data. It is unclear whether the applicant is claiming a data-sink device or further limiting device (2) which renders the claim indefinite. Appropriate correction required.

g. Claim 15 is directed towards a data-source device for making digital data, however, it is dependent on claim 7 which is a device (2) for preventing unwanted use of digital data. It is unclear whether the applicant is claiming a data-source device or further limiting device (2) which renders the claim indefinite. Appropriate correction required.

Claim Rejections - 35 USC § 101

3. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

1. Claims 1-6 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

A claimed process is eligible for patent protection under 35 U.S.C. § 101 if:

> "(1) it is tied to a particular machine or apparatus, or (2) it transforms a particular article into a different state or thing. See Benson, 409 U.S. at 70 (' Transformation and reduction of an article ' to a different state or thing' is the clue to the patentability of a process claim that does not include particular machines.'); Diehr, 450 U.S. at 192 (holding that use of mathematical formula in process ' transforming or reducing an article to a different state or thing' constitutes patent-eligible subject matter); see also Flook, 437 U.S. at 589 n.9 (' An argument can be made [that the Supreme] Court has only recognized a process as within the statutory definition when it either was tied to a particular apparatus or operated to change materials to a ' different state or thing' '); Cochrane v. Deener, 94 U.S. 780, 788 (1876) ('A process is...an act, or a series of acts, performed upon the subject-matter to be transformed and reduced to a different state or thing.').[7] A claimed process involving a

> fundamental principle that uses a particular machine or apparatus would not pre-empt uses of the principle that do not also use the specified machine or apparatus in the manner claimed. And a claimed process that transforms a particular article to a specified different state or thing by applying a fundamental principle would not pre-empt the use of the principle to transform any other article, to transform the same article but in a manner not covered by the claim, or to do anything other than transform the specified article." (*In re Bilski, 88 USPQ2d 1385, 1391 (Fed. Cir. 2008))*

Also noted in *Bilski* is the statement, " Process claim that recites fundamental principle, and that otherwise fails ' machine-or-transformation' test for whether such claim is drawn to patentable subject matter under 35 U.S.C. §101, is not rendered patent eligible by mere field-of-use limitations; another corollary to machine-or-transformation test is that recitation of specific machine or particular transformation of specific article does not transform unpatentable principle into patentable process if recited machine or transformation constitutes mere ' insignificant post-solution activity.' " (*In re Bilski, 88 USPQ2d 1385, 1385 (Fed. Cir. 2008))* Examples of insignificant post-solution activity include data gathering and outputting. Furthermore, the machine or transformation must impose meaningful limits on the scope of the method claims in order to pass the machine-or-transformation test.

It is also noted that the mere recitation of a machine in the preamble in a manner such that the machine fails to patentably limit the scope of the claim does not make the claim statutory under 35 U.S.C. § 101, as seen in the Board of Patent Appeals Informative Opinion *Ex parte Langemyr et al.* (Appeal 2008-1495).

Claims 1-6 are not tied to a particular machine or apparatus nor do they transform a particular article into a different state or thing, thereby failing the machine-or-transformation test.

In particular, a method claim must meet a specialized, limited meaning to qualify as a patent-eligible process claim. The test for a method is whether the claimed method is (1) tied to a particular machine or apparatus. In addition, mere field of use limitations or limitations reciting insignificant extra-solution activity will not transform an unpatentable process into a patentable one as the machine or transformation must impose meaningful limits on the method claim' s scope. This means that reciting a particular machine or transformation in an insignificant step (e.g. data gathering, outputting, displaying, receiving, and the like) will not move to make an unpatentable process patentable.

Claims 1-6 as recited, are directed toward a method for preventing unwanted use of digital data steps of making available of information and withdrawal of the availability of information. As currently written the steps recited in claims 1-6 are not tied to a machine, much less a significant tie to a particular machine, imposing meaningful limits.

Claims 1-6 are therefore non-statutory under § 101. Appropriate correction is required.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. The factual inquiries set forth in *Graham* v. *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

6. Claims 1-17 rejected under 35 U.S.C. 103(a) as being unpatentable over Stefik et al. (US 5,629,980) in view of Ginter et al. (US 5,917,912).

CLAIM 1 –

As per claim 1, Stefik disclose *a* method for preventing the unwanted use of digital data (DI, D2; DI' D2') having the limitations of:

- *which digital data (DI, D2; DI' D2') is available in encoded form,* (col. 9, ll. 45-50...data in the contents file may be..encrypted)
- *which digital data (DI, D2; DI' D2') is made accessible by a data-source device (4) to a data-sink device (3)* (see col. 4, ll. 5-15…repository has two primary operating modes, a server mode and a requester mode) *and*
- *which digital data (DI, D2; DI' D2') has associated with it blocking information (BLI, BL2; BLI', BL2') by means of which any making available of the digital data (DI, D2; DI' D2') by the data-sink device (3) to a further data-sink device can be blocked,* (see col. 6, ll. 40-45...usage rights...rights define how a digital work can be used and if it can be further distributed)
- *which method comprises the method steps specified below, namely,*
- *making available of authorization-to-use information (BBII, BBI2; BBII', BBI2') to a data-sink device (3),* (see col. 17, ll. 64-67...usage right language to define rights associated with digital works and their parts; col 34, ll. 54-60…server transmits the …data to the client according to transmission protocol)

- *which authorization-to-use information (BBII, BBI2; BBII', BBI2') is intended for authorizing the use of the digital data (DI, D2; DI' D2') by the data-sink device (3) and comprises at least the blocking information (BLI, BL2; BLI', BL2') plus decoding information (DCI, DC2; DCI' DC2'),* (see col. 17, ll. 64-67…usage rights statements are interpreted by repositories and are used to determine what transactions can be successfully carried out for a digital work and to determine parameters for those transactions; col. 27, ll. 5-30...writing keys are used to encrypt data and checking keys are used to decrypt data. both writing keys and checking keys may be public or private)
- *which decoding information (DCI, DC2; DCI' DC2') is associated with the digital data (DI, D2; DI' D2'), with which decoding information (DCI, DC2; DCI' DC2') the digital data (DI, D2; DI' D2') can be decoded,* (see col. 27, ll. 5-30…communication can only be read by the private checking key for decryption; col. 41, ll. 40-50...authorization transactions...usage right can specify an authorization-ID which identifies an authorization object (a digital work in a file of a standard format) *and*
- *which decoding information (DCI,DC2; DCI' DC2') is available to the data-source device (4) before the authorization-to-use information (BBII, BBI2; BBII', BBI2') is made available to the data-sink device (3),* (see col. 7, ll. 5-15…create digital work…determine appropriate usage rights..attach them to the digital work and store them in repository 1…if access is granted, repository 1 transmits the digital work to repository 2; col 42, ll. 5-10…authorization server plays the authorization..decrypting it using either the public key of the master repository…or session key; col. 29, ll. 1-10...repository 1 creates a session key pair...second key is a public key used by repository 2 to decrypt messages...second key is...sent to repository 2) *and*
- *withdrawal of the availability of the decoding information (DCI, DC2; DCI' DC2') to the data-source device (4).*(see col. 35, ll. 25-30…number of copies remaining in the server is now zero, it erases the digital work from its memory)

Stefik does not explicitly disclose:

- *which authorization-to-use information (BBII, BBI2; BBII', BBI2') is made available separately from the digital data (DI, D2; DI' D2'),*

Ginter et al. teach(s) content control information may be partially or fully delivered separately from its associated content (see col 17, ll. 45-50). It would have been obvious to one of ordinary skill in the art at the time of the invention to expand the method of Stefik to include separate delivery of content control information as taught by Ginter et al. One of ordinary skill in the art at the time of the invention would

have been motivated to expand the method of Stefik since it provides a flexible, efficient and low cost distribution method of content and content control.

CLAIM 2 –

Stefik in view of Ginter teach(s) the method of claim 1 as described above. Stefik further disclose(s) *a* method for preventing unwanted use of digital data having the limitations of:

- *wherein the withdrawal of the availability of the decoding information (DCI, DC2; DCI' DC2') to the data-source device (4) is performed by deleting the decoding information (DCI, DC2; DCI' DC2') available to the data-source device (3).* (see col. 35, ll. 25-30…number of copies remaining in the server is now zero, it erases the digital work from its memory)

CLAIM 3 –

Stefik in view of Ginter teach(s) the method of claim 1 as described above. Stefik further disclose(s) *a* method for preventing unwanted use of digital data having the limitations of:

- *wherein note is also taken of data-sink information (SO) by means of which the data-sink device (3) can be identified.* (see col. 8, ll. 5-10…identification certificates are the mean by which a repository is identified as "trustworthy")

CLAIM 4 –

Stefik in view of Ginter teach(s) the method of claim 1 as described above. Stefik further disclose(s) *a* method for preventing unwanted use of digital data having the limitations of:

- *wherein the making available of the authorization-to-use information (BBII, BBI2; BBII', BBI2') to the data-sink device (3) and the withdrawal of the availability of the decoding information (DCI, DC2; DCI', DC2') to the data-source device (4) is able to be instigated, as a function of first relationship information (RII) by means of which the relationship between a user (7) of the data-source device (4) and a user (6) of the data-sink device (3) can be defined, either only by the user (7) of the data-source device (4) or by the user (6) of the data-sink device (3) as well.* (see col. 29, ll. 40-50…login transaction is used to check the authenticity of a user requesting a transaction; col. 16, ll. 60-67...user interface must permit a user to input information such as

access requests and alpha numeric data...will then cause the repository to initiate the suitable transactions)

CLAIM 5 –

Stefik in view of Ginter teach(s) the method of claim 1 as described above. Stefik further disclose(s) *a* method for preventing unwanted use of digital data having the limitations of:

- *wherein termination of the making available of the digital data (DI, D2; DI' D2') to the data-sink device (3) comprises firstly the making available to the data-source device (4) of the decoding information (DCI, DC2; DCI' DC2') that was previously made available to the data-sink device (3)* (see col. 36, ll. 20-30…server decrements the copies-in-use field…work….returned automatically) *and*
- *secondly the withdrawal of the availability of the decoding information (DCI, DC2; DCI' DC2') to the data-sink device (3)* . (see col. 36, ll. 20-30…requester…terminates all current uses and erases the digital work copies from memory)

CLAIM 6 –

Stefik in view of Ginter teach(s) the method of claim 5 as described above. Stefik further disclose(s) *a* method for preventing unwanted use of digital data having the limitations of:

- *wherein the termination of the availability of the digital data (DI, D2; DI' D2') to a data-sink device (3) is performed, as a function of second relationship information (RI2) by means of which a relationship between a user (7) of the data-source device (4) and a user (6) of the data-sink device (3) can be defined, either only by the user (6) of the data-sink device (3) or by the user (7) of the data-source device (4) as well.* (see col. 29, ll. 40-50…login transaction is used to check the authenticity of a user requesting a transaction; col. 16, ll. 60-67...user interface must permit a user to input information such as access requests and alpha numeric data...will then cause the repository to initiate the suitable transactions)

CLAIM 7 –

As per claim 7, Stefik disclose *a* device (repository) for preventing unwanted use of digital data (DI, D2; DI' D2') having the limitations of:

- *which digital data (DI, D2; DI' D2') is available in encoded form,* (col. 9, ll. 45-50...data in the contents file may be..encrypted)
- *which digital data (DI, D2; DI' D2') can be made accessible by a data-source device (4) to a data-sink device (3)* (see col. 4, ll. 5-15…repository has two primary operating modes, a server mode and a requester mode) *and*
- *which digital data (DI, D2; DI' D2') has associated with it blocking information (BLI, BL2; BLI', BL2') by means of which any making available of the digital data (DI, D2; DI' D2') by the data-sink device (3) to a further data-sink device can be blocked,* (see col. 6, ll. 40-45...usage rights...rights define how a digital work can be used and if it can be further distributed)
- *wherein management means (9) are provided, which management means (9) are arranged to make available authorization- to-use information (BBII, BBI2; BBII', BBI2') to a data-sink device (3), which authorization-to-use information (BBII, BBI2; BBII', RRT~') is intended for authorizing the use of the digital data (DI, D2;DI' D2') by the data-sink device (3) and comprises at least the blocking information (BLI, BL2; BLI', BL2') plus decoding information (DCI, DC2; DCI' DC2'),* (see col. 17, ll. 64-67…usage rights statements are interpreted by repositories and are used to determine what transactions can be successfully carried out for a digital work and to determine parameters for those transactions; col. 27, ll. 5-30...writing keys are used to encrypt data and checking keys are used to decrypt data. both writing keys and checking keys may be public or private)
- *which decoding information (DCI, DC2; DCI' DC2') is associated with the digital data (DI, D2; DI' D2'), with which decoding information (DCI, DC2; DCI' DC2') the digital data (DI, D2; DI' D2') can be decoded,* (see col. 27, ll. 5-30…communication can only be read by the private checking key for decryption; col. 41, ll. 40-50...authorization transactions...usage right can specify an authorization-ID …a digital work; col. 42, ll. 5-10...server…decrypting it using the public key...or session key) *and*
- *which decoding information (DCI, DC2; DCI' DC2') is available to the data-source device (4) before the authorization-to-use information (BBII, BBI2; BBII', BBI2') is made available to the data-sink device (3),* (see col. 7, ll. 5-15…create digital work…determine appropriate usage rights..attach them to the digital work and store them in repository 1…if access is granted, repository 1 transmits the digital work to repository 2; col 42, ll. 5-10…authorization server plays the authorization..decrypting it using either the public key of the master repository…or session key; col. 29, ll. 1-10...repository 1 creates a session key pair...second key is a public key used by repository 2 to decrypt messages...second key is...sent to repository 2) *and*

- *wherein the management means (9) are arranged to withdraw the availability of the decoding information (DCI, DC2; DCI' DC2') to the data-source device (4).* (see col. 35, ll. 25-30…erases the digital work from its memory)

Stefik does not explicitly disclose:

- *which authorization-to-use information (BBII, BBI2; BBII', BBI2') exists separately from the digital data (DI, D2; DI' D2'),*

Ginter et al. teach(s) content control information may be partially or fully delivered separately from its associated content (see col 17, ll. 45-50). It would have been obvious to one of ordinary skill in the art at the time of the invention to expand the system of Stefik to include separate delivery of content control information as taught by Ginter et al. One of ordinary skill in the art at the time of the invention would have been motivated to expand the system of Stefik since it provides a flexible, efficient and low cost distribution method of content and content control.

CLAIM 8 –

Stefik in view of Ginter teach(s) the device of claim 7, as described above. Ginter further disclose(s) *a* device for preventing unwanted use of digital data having the limitations of:

- *wherein, for withdrawing the availability of the decoding information (DCI, DC2; DCI' DC2') to the data-source device (4), the management means (9) are arranged to delete the decoding information (DCI, DC2; DCI' DC2') available to the data-source device (4).* (see col. 35, ll. 25-30…erases the digital work from its memory)

CLAIM 9 –

Stefik in view of Ginter teach(s) the device of claim 7, as described above. Stefik further disclose(s) *a* device for preventing unwanted use of digital data having the limitations of:

- *wherein the management means (9) are, in addition, arranged to take note of data-sink information (SO) for the data-source device (4) by means of which the data-sink device (3) can be identified.* (see col. 8, ll. 5-10…identification certificates are the means by which a repository is identified as "trustworthy")

CLAIM 10 –

Stefik in view of Ginter teach(s) the device of claim 7 as described above. Stefik further disclose(s) *a*

device for preventing unwanted use of digital data having the limitations of:

- *wherein the management means (9) are, in addition, arranged to take account of first relationship information (RII) by means of which a relationship between a user (7) of the data-source device (4) and a user of the data-sink device (3) can be defined,* (see col. 29, ll. 40-50…login transaction is used to check the authenticity of a user requesting a transaction) *and*
- *wherein the management means (9) are arranged, as a function of the relationship defined by the first relationship information (RII), to enable the making available of the authorization-to-use information (BBII, BBI2; BBII', BBI2') to the data-sink device (3) and the withdrawal of the availability of the decoding information (DCI, DC2; DCI' DC2') to the data-source device (4) to take place either only at the instigation of the user (7) of the data-source device (4) or at the instigation of the user (6) of the data-sink device (3) as well.* (see col. 16, ll. 60-67...user interface must permit a user to input information such as access requests and alpha numeric data...will then cause the repository to initiate the suitable transactions)

CLAIM 11 –

Stefik in view of Ginter teach(s) the device of claim 7 as described above. Stefik further disclose(s) *a*

device for preventing unwanted use of digital data having the limitations of:

- *wherein, for termination of the availability of the digital data (DI, D2; DI' D2') to the data-sink device (3), the management means (9) are arranged to make available to the data-source device (4) the decoding information (DCI, DC2; DCI' DC2') that was previously made available to the data-sink device (3) (DCI, DC2; DCI' DC2') that was previously made available to the data-sink device (3)* (see col. 36, ll. 20-30…server decrements the copies-in-use field…work….returned automatically) *and*
- *to withdraw the availability of the decoding information (DCI, DC2; DCI' DC2') to the data-sink device (3).* (see col. 36, ll. 20-30…requester…terminates all current uses and erases the digital work copies from memory)

CLAIM 12 –

Stefik in view of Ginter teach(s) the device of claim 11 as described above. Stefik further disclose(s) *a*

device for preventing unwanted use of digital data having the limitations of:

- *wherein the management means (9) are, in addition, arranged to take account of second relationship information (RI2) by means of which a relationship between a user (7) of the data-source device (4) and a user (6) of the data-sink device (3) can be defined,* (see col. 29, ll. 40-50…login transaction is used to check the authenticity of a user requesting a transaction) *and*
- *wherein the management means (9) are arranged, as a function of the relationship defined by the second relationship information (RI2) to enable the termination of the availability of the digital data (DI, D2; DI' D2') to the data-sink device (3) to take place either only at the instigation of the user (6) of the data-sink device (3) or at the instigation of the user (7) of the data-source device (4) as well.* (see col. 16, ll. 60-67...user interface must permit a user to input information such as access requests and alpha numeric data...will then cause the repository to initiate the suitable transactions)

CLAIM 13 –

Stefik in view of Ginter teach(s) the device of claim 7 as described above. Stefik further disclose(s) *a* device for preventing unwanted use of digital data having the limitations of:

- *A data-sink device (3)* (repository) *for using digital data, which digital data (DI, D2; DI' D2') is available in encoded form,* (col. 9, ll. 45-50...data in the contents file may be..encrypted)
- *which digital data (DI, D2; DI' D2') can be made accessible by a data-source device (4) to the data-sink device (3)* (see col. 265, ll. 48-55...transactions occur between two repositories) *and*
- *which digital data (DI, D2; DI' D2') has associated with it blocking information (BLI, BL2; BLI', BL2') by means of which any making available of the digital data (DI, D2; DI' D2') by the data-sink device (3) to a further data-sink device can be blocked,* (see col. 6, ll. 40-45...usage rights...rights define how a digital work can be used and if it can be further distributed)
- *wherein first processing means (16) are provided that are arranged to process the digital data (DI, D2; DI' D2') by taking account of a first enabling signal (ESI) able to be fed to them,* (see col 14, ll. processing means provides controller, repository transaction and usage rights transaction functions for the repository; col 14, ll. 45-50...external interface means provides for the signal connection to other repositories)
- *which first enabling signal (ESI) enables the digital data (DI, D2; DI' D2') to be processed by the first processing means,* (see col. 14, ll. 45-50…provides for the exchange of signals) *and*
- *by using decoding information (DCI, DC2; DCI' DC2'), which decoding information (DCI, DC2; DCI' DC2') is associated with the digital data (DI, D2; DI' D2') and the digital data (DI, D2; DI' D2') can be decoded by means thereof,* (see col. 14, ll. 10-20...decryption and/or decompression of digital works and transaction messages are also performed by the processing means)

- *wherein first checking means (15) are provided that are arranged firstly to cooperate with a device (2) as claimed in claim 7, that are arranged secondly to check whether authorization-to-use information (BBII, BBI2; BBII', BBI2') is available for the data-sink device (3),* (see col. 8-16..usage transaction handler comprise functionality for processing access requests to digital works)
- *which authorization-to- use information (BBII, BBI2; BBII', BBI2') is intended for authorizing the use of the digital data (DI, D2; DI' D2') by the data-sink device (3), comprises at least the blocking information (BLI, BL2; BLI', BL2') and the decoding information (DCI, DC2; DCI' DC2') and is available to the data-source device (4) before it is made available to the data-sink device (3),* (see col. 17, ll. 64-67…usage rights statements are interpreted by repositories and are used to determine what transactions can be successfully carried out for a digital work and to determine parameters for those transactions; col. 41, ll. 40-50…usage right can specify an authorization-ID…a digital work…server...decrypting it using...public key...or the session key; col. 27, ll. 5-30...writing keys are used to encrypt data and checking keys are used to decrypt data. both writing keys and checking keys may be public or private) *and*
- *that are arranged thirdly to generate the first enabling signal (ESI) and transmit the first enabling signal (ESI) to the processing means (16) when there is a positive result to the check,* (see fig. 12; col. 14, ll. 45-50...signal connection) *and*
- *wherein first blocking means (18) are provided that, by taking account of the blocking information (BLI, BL2; BLI', BL2'), are arranged to block any making available of the digital data (DI, D2; DI' D2') to a further data-sink device.* (see col. 14, ll. 62-68...core repository services...controlling the distribution and use of digital works)

Stefik does not explicitly disclose:

- *which authorization-to-use information (BBII, BBI2; BBII', BBI2') exists separately from the digital data (DI, D2; DI' D2'),*

Ginter et al. teach(s) content control information may be partially or fully delivered separately from its associated content (see col 17, ll. 45-50). It would have been obvious to one of ordinary skill in the art at the time of the invention to expand the system of Stefik to include separate delivery of content control information as taught by Ginter et al. One of ordinary skill in the art at the time of the invention would have been motivated to expand the system of Stefik since it provides a flexible, efficient and low cost distribution method of content and content control.

CLAIM 14 –

Stefik in view of Ginter teach(s) the device of claim 13 as described above. Stefik further disclose(s) *a* device for preventing unwanted use of digital data having the limitations of:

- *which data-sink device (3) contains a device (2) for preventing unwanted use of digital data (DI, D2; DI' D2'), which digital data (DI, D2; DI', D2') is available in encoded form,* (see col 13, ll. 45-50..repositories may be devices..or may be incorporated into other systems; col. 9, ll. 45-50...data in the contents file may be..encrypted)
- *which digital data (DI, D2; DI' D2') can be made accessible by a data-source device (4) to a data-sink device (3)* (see col. 265, ll. 48-55...transactions occur between two repositories) *and*
- *which digital data (DI, D2; DI' D2') has associated with it blocking information (BLI, BL2; BLI', BL2') by means of which any making available of the digital data (DI, D2;DI' D2') by the data-sink device (3) to a further data-sink device can be blocked,* (see col. 6, ll. 40-45...usage rights...rights define how a digital work can be used and if it can be further distributed)
- *wherein management means (9) are provided, which management means (9) are arranged to make available authorization- to-use information (BBII, BBI2; BBII', BBI2') to a data-sink device (3), which authorization-to-use information (BBII, BBI2; BBII', BBI2') is intended for authorizing the use of the digital data (Di, D2;DI' D2') by the data-sink device (3) and comprises at least the blocking information (BLI, BL2; BLI', BL2') plus decoding information (DCI, DC2; DCI' DC2'),* (see col. 17, ll. 64-67…usage rights statements are interpreted by repositories and are used to determine what transactions can be successfully carried out for a digital work and to determine parameters for those transactions; col. 27, ll. 5-30...writing keys are used to encrypt data and checking keys are used to decrypt data. both writing keys and checking keys may be public or private)
- *which decoding information (DCI, DC2; DCI' DC2') is associated with the digital data (DI, D2; DI' D2'), and with which decoding information (DCI, DC2; DCI' DC2') the digital data (DI, D2; DI' D2') can be decoded,* (see col. 27, ll. 5-30…communication can only be read by the private checking key for decryption; col. 41, ll. 40-50...authorization transactions...usage right can specify an authorization-ID which identifies an authorization object (a digital work in a file of a standard format) *and*
- *which decoding information (DCI, DC2; DCI' DC2') is available to the data-source device (4) before the authorization-to-use information (BBII, BBI2; BBII', BBI2') is made available to the data-sink device (3),* (see col. 7, ll. 5-15…create digital work…determine appropriate usage rights..attach them to the digital work and store them in repository 1…if access is granted,

repository 1 transmits the digital work to repository 2; col 42, ll. 5-10…authorization server plays the authorization..decrypting it using either the public key of the master repository…or session key; col. 29, ll. 1-10...repository 1 creates a session key pair...second key is a public key used by repository 2 to decrypt messages...second key is...sent to repository 2) *and*

- *wherein the management means (9) are arranged to withdraw the availability of the decoding information DCI, DC2; DCI' DC2') to the data-source device (4).* (see col. 35, ll. 25-30…erases the digital work from its memory (see col. 35, ll. 25-30…erases the digital work from its memory)

Stefik does not explicitly disclose:

- *which authorization-to-use information (BBII, BBI2; BBII', BBI2') exists separately from the digital data (DI, D2; DI' D2'),*

Ginter et al. teach(s) content control information may be partially or fully delivered separately from its associated content (see col 17, ll. 45-50). It would have been obvious to one of ordinary skill in the art at the time of the invention to expand the system of Stefik to include separate delivery of content control information as taught by Ginter et al. One of ordinary skill in the art at the time of the invention would have been motivated to expand the system of Stefik since it provides a flexible, efficient and low cost distribution method of content and content control.

CLAIM 15 –

Stefik in view of Ginter teach(s) the device of claim 7 as described above. Stefik further disclose(s) *a* device for preventing unwanted use of digital data having the limitations of:

- *A data-source device (4)* (repository) *for making digital data (DI, D2; DI' D2') available to a data-sink device (3),* (see col 7, ll. 44-46...repository has two modes of operation a server mode and a requester mode)
- *which digital data (DI, D2; DI' D2') is available in encoded form* (see col. 9, ll. 45-50...data in the contents file may be..encrypted) *and*
- *which digital data (DI, D2; DI' D2') has associated with it blocking information (BLI, BL2; BLI', BL2') by means of which any making available of the digital data (DI, D2; DI' D2') by the data-sink device (3) to a further data-sink device (3) can be blocked,* (see col. 6, ll. 40-45...usage rights...rights define how a digital work can be used and if it can be further distributed)

- *wherein second processing means (22) are provided that are arranged to process the digital data (DI, D2; DI' D2') by taking account of a second enabling signal (ES2) able to be fed to them,* (see col 14, ll. processing means provides controller, repository transaction and usage rights transaction functions for the repository; col 14, ll. 45-50...external interface means provides for the signal connection to other repositories)
- *which second enabling signal (ES2) enables the digital data (DI, D2; DI' D2')* to *be processed by the second processing means (22),* (col. 14, ll. 40-50…provides for the exchange of signals via such standard interface) *and*
- *by using decoding information (DCI, DC2; DCI' DC2'), which decoding information (DCI, DC2; DCI' DC2') is associated with the digital data (DI, D2; DI' D2') and the digital data (DI, D2; DI' D2') can be decoded by means thereof,* (see col. 14, ll. 10-20...decryption and/or decompression of digital works and transaction messages are also performed by the processing means) *and*
- *wherein second checking means (21) are provided that are arranged firstly to cooperate with a device (2) as claimed in claim 7, that are arranged secondly to check whether decoding information (DCI, DC2; DCI', DC2') is available for the data-source device (4),* (see col. 8-16..usage transaction handler comprise functionality for processing access requests to digital works) *and*
- *that are arranged thirdly to generate the second enabling signal (ES2) and transmit the second enabling signal (ES2) to the second processing means (22) when there is a positive result to the check.* (see col. 14, ll. 45-50...signal connection; col. 14, ll. 62-68...core repository services...controlling the distribution and use of digital works)

CLAIM 16 –

Stefik in view of Ginter teach(s) the device of claim 16 as described above. Stefik further disclose(s) *a*

device for preventing unwanted use of digital data having the limitations of:

- *A data-source device (4) which contains a device (2) for preventing unwanted use of digital data (DI, D2; DI' D2'), which digital data (DI, D2; DI' D2') is available in encoded form,* (see col 13, ll. 45-50..repositories may be devices..or may be incorporated into other systems; col. 9, ll. 45-50...data in the contents file may be..encrypted)
- *which digital data (DI, D2; DI' D2') can be made accessible by a data-source device (4) to a data-sink device (3)* (see col 7, ll. 44-46...repository has two modes of operation a server mode and a requester mode) *and*
- *which digital data (DI, D2; DI' D2') has associated with it blocking information (BLI, BL2; BLI', BL2') by means of which any making available of the digital data (DI, D2; DI' D2') by the data-sink*

device (3) to a further data-sink device can be blocked, (see col. 6, ll. 40-45...usage rights...rights define how a digital work can be used and if it can be further distributed)

- *wherein management means (9) are provided, which management means (9) are arranged to make available authorization- to-use information (BBII, BBI2; BBII', BBI2') to a data-sink device (3), which authorization-to-use information (BBII, BBI2; BBII', BBI2') is intended for authorizing the use of the digital data (DI, D2;DI' D2') by the data-sink device (3) and comprises at least the blocking information (BLI, BL2; BLI', BL2') plus decoding information (DCI, DC2; DCI' DC2'),*(see col. 17, ll. 64-67…usage rights statements are interpreted by repositories and are used to determine what transactions can be successfully carried out for a digital work and to determine parameters for those transactions; col. 27, ll. 5-30...writing keys are used to encrypt data and checking keys are used to decrypt data. both writing keys and checking keys may be public or private)
- *which decoding information (DCI,DC2; DCI' DC2') is associated with the digital data (DI, D2; DI' D2'), and with which decoding information (DCI, DC2; DCI' DC2') the digital data (DI, D2; DI' D2') can be decoded,* (see col. 27, ll. 5-30…communication can only be read by the private checking key for decryption; col. 41, ll. 40-50...authorization transactions...usage right can specify an authorization-ID which identifies an authorization object (a digital work in a file of a standard format) *and*
- *which decoding information (DCI, DC2; DCI' DC2') is available to the data-source device (4) before the authorization-to-use information (BBII, BBI2; BBII', BBI2') is made available to the data-sink device (3)* (see col. 7, ll. 5-15…create digital work…determine appropriate usage rights..attach them to the digital work and store them in repository 1…if access is granted, repository 1 transmits the digital work to repository 2; col 42, ll. 5-10…authorization server plays the authorization..decrypting it using either the public key of the master repository…or session key; col. 29, ll. 1-10...repository 1 creates a session key pair...second key is a public key used by repository 2 to decrypt messages...second key is...sent to repository 2) *, and*
- *wherein the management means (9) are arranged to withdraw the availability of the decoding information (DCI, DC2; DCI' DC2') to the data-source device (4).* (see col. 35, ll. 25-30…erases the digital work from its memory)

Stefik does not explicitly disclose:

- *which authorization-to-use information (BBII, BBI2; BBII', BBI2') exists separately from the digital data (DI, D2; DI' D2'),*

Ginter et al. teach(s) content control information may be partially or fully delivered separately from its associated content (see col 17, ll. 45-50). It would have been obvious to one of ordinary skill in the art at the time of the invention to expand the system of Stefik to include separate delivery of content control information as taught by Ginter et al. One of ordinary skill in the art at the time of the invention would have been motivated to expand the system of Stefik since it provides a flexible, efficient and low cost distribution method of content and content control.

CLAIM 17 –
Stefik in view of Ginter teach(s) the device of claim 13 as described above. Stefik further disclose(s) *a* device for preventing unwanted use of digital data having the limitations of:

- *A combination device (24, 25) having a data-source device and a data-sink device, which combination device (24, 25) contains a data-source device (4) as claimed claim 13.* (see fig. 2; col. 7, ll. 44-46…repository has two modes of operation; a server mode and a requester mode; col. 13, ll. 45-50…repositories may be devices..or may be incorporated into other systems)

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Banerjee et al. (US 2003/0004885). Banerjee is pertinent since it disclose a method and system for digital rights management including secure distribution and flexible content privileges.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to ALEXIS WELLS whose telephone number is (571) 270-7784. The examiner can normally be reached on Monday - Thursday, 8:00 - 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner' s supervisor, Andrew Fischer can be reached on (571) 272-6779. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

//amw//

/EVENS J. AUGUSTIN/
Primary Examiner, Art Unit 3621